Strong no-go theorem for Gaussian quantum bit commitment

Loïck Magnin, Frédéric Magniez, Anthony Leverrier, Nicolas J. Cerf

PHYSICAL REVIEW A **81**, 010302(R) (2010)

Strong no-go theorem for Gaussian quantum bit commitment

Loïck Magnin,[1,2] Frédéric Magniez,[2] Anthony Leverrier,[3] and Nicolas J. Cerf[1,4]

[1]*Quantum Information and Communication (QuIC), École Polytechnique, Université Libre de Bruxelles, B-1050 Brussels, Belgium*

[2]*Laboratoire de Recherche en Informatique (LRI), Univ Paris-Sud, CNRS, F-91405 Orsay, France*

[3]*Institut Telecom / Telecom ParisTech, CNRS LTCI, 46 rue Barrault, F-75634 Paris Cedex 13, France*

[4]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 22 May 2009; published 6 January 2010)

Unconditionally secure bit commitment is forbidden by quantum mechanics. We extend this no-go theorem to continuous-variable protocols where both players are restricted to use Gaussian states and operations, which is a reasonable assumption in current-state optical implementations. Our Gaussian no-go theorem also provides a natural counter-example to a conjecture that quantum mechanics can be rederived from the assumption that key distribution is allowed while bit commitment is forbidden in Nature.

DOI: 10.1103/PhysRevA.81.010302 PACS number(s): 03.67.Dd

Bit commitment is a cryptographic primitive with a large scope of applications ranging from two-party secure computation, e.g., secure authentication, to coin flipping. It involves two mistrustful parties: Alice must commit to a certain bit, which should remain hidden to Bob until she reveals its value. A traditional picture for this protocol is as follows: Alice locks a secret bit into a safe that she gives to Bob; then, when she wants to reveal her secret, she simply hands over the key of the safe to Bob. A bit commitment protocol is said to be secure if it prevents Alice from cheating (i.e., she cannot change the value of the bit she has committed) and Bob from cheating (i.e., he cannot learn information about the bit before Alice reveals it).

This primitive has been exhaustively studied in classical cryptography, where the security relies on unproven computational assumptions [1,2]. The idea of quantum bit commitment (QBC) was first introduced by Bennett and Brassard in 1984 [3], together with the famous BB84 quantum key distribution protocol. In 1993, Brassard *et al.* proposed a QBC protocol known as the Brassard-Crepeau-Jozsa-Langlois (BCJL) protocol [4], which was believed to be secure until 1996, when Mayers [5] and independently Lo and Chau [6] proved that it was not the case. Their proof involved a reduction of the BCJL protocol to a purified protocol, which cannot be perfectly secure against both Alice and Bob. Thus, it appeared that this reduction precludes the existence of an unconditionally secure QBC protocol. Because of the complexity of this reduction, however, it was not universally accepted (see, e.g., [7]) until 2006, when d'Ariano *et al.* provided a complete, formal description of QBC protocols that definitely closed the question [8]. This is the content of the *no-go theorem* for QBC.

Interestingly, this situation is in sharp contrast with quantum key distribution, for which unconditionally secure protocols have been exhibited [9]. These two facts, namely, the possibility of key distribution and impossibility of bit commitment, seem to be specific to quantum mechanics and were conjectured by Brassard and Fuchs to be actually sufficient to rederive quantum mechanics from first principles [10]. This conjecture was later proven wrong, but Clifton *et al.* proved instead that the assumptions of no signaling, no broadcasting, and the impossibility of bit commitment make it work within the framework of C^* algebras [11]. This is known as the Clifton-Bub-Halvorson (CBH) theorem.

Coming back to the no-go theorem for QBC, let us stress that it only applies to unconditionally secure protocols, that is, to the case where Alice and Bob have no restriction on their capabilities except those dictated by quantum mechanics. This leaves the door open to QBC protocols that could be secure under reasonable assumptions on Alice and Bob's capabilities. Such protocols were found in the bounded-storage model [12] or by exploiting the constraints imposed by special relativity [13].

In this Rapid Communication, we address QBC protocols with *continuous variables*, and explore whether such protocols may be found secure when both parties are restricted to use Gaussian states and operations. Most quantum information protocols to date have been based on discrete variables in a finite-dimensional Hilbert space. Recently, however, continuous variables (CVs) have been proven to be a very powerful alternative approach [14]. In the case of optical communication, for example, the quadrature components of the light field make especially useful continuous variables because of their associated detection scheme, namely, homodyne detection. This is well illustrated with CV quantum key distribution, which was recently proven unconditionally secure [15] and appears as a credible alternative to single-photon-based quantum key distribution [16]. Dealing with CV quantum information protocols unfortunately comes with a price, namely, that their analysis may be intractable because an infinite-dimensional Hilbert space is involved.

An elegant solution consists in restricting the analysis to so-called Gaussian states and operations, which, apart from being efficiently characterizable within the appropriate formalism, can be relatively easily manipulated in the laboratory. It is therefore a very natural and important question to ask whether QBC protocols can be built with continuous variables, which could be made secure if both parties are capable of manipulating Gaussian states only. Remember that although the no-go theorem for unconditional security holds for infinite-dimensional Hilbert spaces as such, it is unknown whether secure QBC can exist when both parties have restricted capabilities. Here, we answer by the negative if this restriction is put at the boundary of the set of Gaussian

states, and we establish a *strong* no-go theorem for Gaussian QBC protocols. Specifically, for any Gaussian QBC protocol, we find a corresponding Gaussian cheating strategy. Moreover, we provide a constructive attack for any CV QBC protocol, whereas constructive attacks were previously known for finite dimensions only.

Let us first recall some notions linked to the distinguishability of quantum states. The *fidelity* between two states ρ and σ is defined as $\mathcal{F}(\rho,\sigma)=(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2$. If $\rho=|\psi\rangle\langle\psi|$ and $\sigma=|\phi\rangle\langle\phi|$ are pure states, the fidelity is simply $|\langle\psi|\phi\rangle|^2$. Any purifications $|\psi\rangle$ of ρ and $|\phi\rangle$ of σ satisfy $\mathcal{F}(\psi,\phi)\leqslant\mathcal{F}(\rho,\sigma)$. Uhlmann's theorem [17] states that this inequality can always be saturated, that is, there exists a purification of ρ (σ) noted $|\psi'\rangle$ ($|\phi'\rangle$) which is such that $\mathcal{F}(\psi',\phi')=\mathcal{F}(\rho,\sigma)$. Although this has been shown regardless of the dimension, constructive proofs of this purification are known in finite dimensions only [18]. The *trace distance* between the states ρ and σ is defined as $D(\rho,\sigma)=\frac{1}{2}\|\rho-\sigma\|_1$, where $\|\tau\|_1=\mathrm{Tr}\sqrt{\tau^\dagger\tau}$ for any operator τ. The trace distance is related to the *guessing probability* $\frac{1}{2}[1+D(\rho,\sigma)]$, which is the maximum probability of distinguishing the two states with the best measurement. We also recall a useful relation between the fidelity and trace distance,

$$D(\rho,\sigma)\leqslant\sqrt{1-\mathcal{F}(\rho,\sigma)}, \tag{1}$$

as well as the Bhattacharyya bound [19,20], namely,

$$1-D(\rho,\sigma)\leqslant\mathrm{Tr}(\sqrt{\rho}\sqrt{\sigma}). \tag{2}$$

Quantum bit commitment. Formally, any (reduced) QBC protocol can be described as follows: Alice encodes her bit b into a pure bipartite state $|\psi_b\rangle$ and sends one half to Bob. At the end of the committing phase, Bob holds either $\rho_0=\mathrm{Tr}_A|\psi_0\rangle\langle\psi_0|$ or $\rho_1=\mathrm{Tr}_A|\psi_1\rangle\langle\psi_1|$ if Alice wants to commit to 0 or 1, respectively. The protocol is referred to as ε-*concealing* if $D(\rho_0,\rho_1)\leqslant\varepsilon$, which means that Bob cannot learn the value of b, except with probability ε. To reveal her bit, Alice sends the other half of $|\psi_b\rangle$. In a so-called δ-*cheating strategy*, Alice sends a state $\rho^\sharp$ in the committing phase and then decides to follow a strategy leading to a final state of her choice, $|\psi_0^\sharp\rangle$ or $|\psi_1^\sharp\rangle$, so that Bob should not be able to distinguish this strategy from an honest strategy with a probability greater than δ. This means that $D(\rho^\sharp,\rho_b)\leqslant\delta$ and $D(\psi_b^\sharp,\psi_b)\leqslant\delta$. Here, we will only consider the simple strategy in which $\rho^\sharp=\rho_0$ and $|\psi_0^\sharp\rangle=|\psi_0\rangle$. Thus, $|\psi_1^\sharp\rangle$ will correspond to Alice initially committing to a zero and then cheating to make it a one. Without loss of generality, we will also consider that $|\psi_b\rangle$ are $2n$-mode states and ρ_b are n-mode states. Now, let us state our main result:

Theorem 1. Given any ε-concealing Gaussian quantum bit commitment protocol to Bob, there exists a Gaussian $\sqrt{2\varepsilon}$-cheating strategy for Alice.

For finite-dimensional protocols, the cheating strategy is usually exhibited with the help of Uhlmann's theorem, which gives purifications $|\psi_0\rangle$ of ρ_0 and $|\psi_1\rangle$ of ρ_1 such that $\mathcal{F}(\psi_0,\psi_1)=\mathcal{F}(\rho_0,\rho_1)$. Unfortunately, it is not known how to use this theorem to explicitly construct such purifications in infinite dimensions, and, even so, it would not help making statements about the Gaussianity of such purifications for Gaussian states. Our approach is based instead on the notion of *intrinsic purification*, for which we give an explicit construction guaranteeing that every Gaussian state has a Gaussian intrinsic purification. Although this purification does not reach Uhlmann's bound, we derive an inequality which is sufficient to prove our theorem:

Lemma 1. Given the n-mode states ρ_0 and ρ_1, there exist $2n$-mode purifications $|\hat{\psi}_0\rangle$ of ρ_0 and $|\hat{\psi}_1\rangle$ of ρ_1 such that

$$D(\hat{\psi}_0,\hat{\psi}_1)\leqslant\sqrt{2\,D(\rho_0,\rho_1)}. \tag{3}$$

Moreover, if ρ_0 and ρ_1 are Gaussian states, so are their purifications $|\hat{\psi}_0\rangle$ and $|\hat{\psi}_1\rangle$.

Gaussian formalism. The state ρ of an n-mode bosonic quantum system is a unit-trace Hermitian positive semidefinite operator on $\mathcal{H}^{\otimes n}$, where $\mathcal{H}$ is the infinite-dimensional Hilbert space spanned by the excitations of each mode. We note $\mathbf{i}=i_1\cdots i_n$ and $|\mathbf{i}\rangle=|i_1\rangle\cdots|i_n\rangle$, where $\{|i\rangle\}$ is the Fock basis of $\mathcal{H}$. Since $\mathcal{H}$ is isomorphic to $\mathcal{L}^2(\mathbb{R})$, any state ρ is completely characterized by its Wigner function W_ρ, a quasiprobability distribution in the $2n$-dimensional phase space parametrized by the vector of quadratures $\xi=(x_1,p_1,\ldots,x_n,p_n)$. The covariance matrix γ of W_ρ is a real, symmetric, and positive matrix satisfying the Heisenberg inequality $\gamma+i\Omega\geqslant 0$, where $\Omega=\bigoplus_{k=1}^n\begin{pmatrix}0&1\\-1&0\end{pmatrix}$. An n-mode state is called Gaussian if its Wigner function is Gaussian, that is,

$$W_\rho(\xi)=\frac{1}{(2\pi)^n\sqrt{\det\gamma}}\exp\left\{-\frac{1}{2}(\xi-\mu)^T\gamma^{-1}(\xi-\mu)\right\}.$$

Note that a Gaussian state is fully described by its first- and second-order moments $\mu\in\mathbb{R}^{2n}$ and $\gamma\in\mathbb{R}^{2n}\times\mathbb{R}^{2n}$.

A *Gaussian operation* $\mathcal{E}$ maps any Gaussian state to a Gaussian state. Therefore, $\mathcal{E}$ is fully characterized by its action on the first- and second-order moments of a state. Furthermore, $\mathcal{E}$ is a Gaussian unitary operator if and only if there exists a symplectic matrix S (such that $S\Omega S^T=\Omega$) and a displacement vector d such that for all states ρ, $W_{\mathcal{E}(\rho)}(\xi)=W_\rho(S^{-1}\xi-d)$ [21]. The Williamson decomposition theorem states that a covariance matrix γ is described by its *symplectic eigenvalues* $\{\nu_1,\ldots,\nu_n\}$. More specifically, for any γ, there exists a symplectic transformation S such that $S\gamma S^T=\bigoplus_{k=1}^n\nu_k\mathbb{I}_2$, with $\nu_k\geqslant 1$ [22]. In particular, for a Gaussian state ρ, there exists a Gaussian operation V, a *Williamson unitary*, such that $V^\dagger\rho V=\sum_{\mathbf{i}}[\prod_{k=1}^n(1-x_k)x_k^{i_k}]|\mathbf{i}\rangle\langle\mathbf{i}|$, where $x_k=\frac{\nu_k-1}{\nu_k+1}$. In other words, any Gaussian state ρ can be mapped via a Gaussian operation V onto a tensor product of thermal states with symplectic eigenvalues ν_k.

Gaussian intrinsic purification. Let ρ be an n-mode state and U a diagonalization of ρ in the Fock basis; that is, U is a unitary operator such that $\langle\mathbf{i}|U^\dagger\rho U|\mathbf{j}\rangle=p_\mathbf{i}\,\delta_{\mathbf{ij}}$, where $\delta_{\mathbf{ij}}$ is the Kronecker delta. We then define an intrinsic purification $|\hat{\psi}\rangle$ of ρ as

$$|\hat{\psi}\rangle=(U^*\otimes U)\sum_{\mathbf{i}}\sqrt{p_\mathbf{i}}|\mathbf{i}\rangle|\mathbf{i}\rangle. \tag{4}$$

(Note that it is not unique.) Here and in what follows, A^* (A^T) denotes the complex conjugate (transpose) of any linear operator A relative to the Fock basis, defined as $\langle\mathbf{i}|A^*|\mathbf{j}\rangle=\langle\mathbf{i}|A|\mathbf{j}\rangle^*$ and $\langle\mathbf{i}|A^T|\mathbf{j}\rangle=\langle\mathbf{j}|A|\mathbf{i}\rangle$.

A Gaussian intrinsic purification of a Gaussian state ρ thus consists of choosing $U = V$, that is, using a Williamson unitary in order to diagonalize ρ in the Fock basis. Let us show that this purification is indeed Gaussian. The state $\sum_{\mathbf{i}} \sqrt{p_{\mathbf{i}}}|\mathbf{i}\rangle|\mathbf{i}\rangle$, being a tensor product of two-mode squeezed states, is Gaussian. Since U is a Gaussian unitary operator, all that is left to show in order to prove that $|\hat{\psi}\rangle$ is a Gaussian state is that U^* is a Gaussian unitary operator too. Let us take an arbitrary n-mode Gaussian state τ and assume that U is described by the symplectic matrix S and displacement vector d. We want to show that applying U^* to τ is equivalent to applying the symplectic matrix $\Sigma_Z^n S^{-1} \Sigma_Z^n$ and the displacement $\Sigma_Z^n d$ in the phase space. We first note that $U^* = (U^\dagger)^T$ and observe that $U^* \tau U^{*\dagger} = (U \tau^T U^\dagger)^T$. The transposition has a simple expression in phase space, namely, for all states σ, $W_{\sigma^T}(\xi) = W_\sigma(\Sigma_Z^n \xi)$, where $\Sigma_Z^n = \bigoplus_{k=1}^n \sigma_Z$ [23]. This leads us to the relation

$$W_{U^* \tau U^{*\dagger}}(\xi) = W_\tau \left(\Sigma_Z^n S^{-1} \Sigma_Z^n \xi - \Sigma_Z^n d \right). \tag{5}$$

To conclude, we observe that $(\Sigma_Z^n S^{-1} \Sigma_Z^n)^{-1} = \Sigma_Z^n S \Sigma_Z^n$ is a symplectic matrix since $\Sigma_Z^n \Omega (\Sigma_Z^n)^T = -\Omega$.

Let us now proceed with the proof of Lemma 1, which is based on the intrinsic purifications $|\hat{\psi}_0\rangle$ and $|\hat{\psi}_1\rangle$ of the n-mode states ρ_0 and ρ_1. We start with the decomposition of $|\psi_b\rangle$ as $|\psi_b\rangle = (U_b^* \otimes U_b) \sum_{\mathbf{i}} \sqrt{p_{b,\mathbf{i}}} |\mathbf{i}\rangle|\mathbf{i}\rangle$. Using the basis $\{U_0|\mathbf{k}\rangle\}_{\mathbf{k}}$, we can write $\mathrm{Tr}(\sqrt{\rho_0}\sqrt{\rho_1})$ as

$$\sum_{\mathbf{i},\mathbf{j},\mathbf{k}} \sqrt{p_{0,\mathbf{i}} p_{1,\mathbf{j}}} \, (\langle \mathbf{k}|U_0^\dagger) U_0 |\mathbf{i}\rangle \langle \mathbf{i}| U_0^\dagger U_1 |\mathbf{j}\rangle \langle \mathbf{j}| U_1^\dagger (U_0|\mathbf{k}\rangle), \tag{6}$$

and the inner product $\langle \psi_0 | \psi_1 \rangle$ as

$$\sum_{\mathbf{i},\mathbf{j}} \sqrt{p_{0,\mathbf{i}} p_{1,\mathbf{j}}} \, \langle \mathbf{i}| (U_0^\dagger U_1)^* |\mathbf{j}\rangle \langle \mathbf{i}| U_0^\dagger U_1 |\mathbf{j}\rangle. \tag{7}$$

Using $|\langle \psi_0 | \psi_1 \rangle| = \sqrt{\mathcal{F}(\psi_0, \psi_1)}$ and the definition of U^*, a straightforward calculation then shows that

$$\mathrm{Tr}(\sqrt{\rho_0}\sqrt{\rho_1}) = \sqrt{\mathcal{F}(\hat{\psi}_0, \hat{\psi}_1)}. \tag{8}$$

Combining Eq. (8) with inequality (2) gives

$$1 - D(\rho_0, \rho_1) \leqslant \sqrt{\mathcal{F}(\hat{\psi}_0, \hat{\psi}_1)}, \tag{9}$$

which, together with inequality (1), yields

$$D(\hat{\psi}_0, \hat{\psi}_1) \leqslant \sqrt{2\, D(\rho_0, \rho_1) - D(\rho_0, \rho_1)^2}. \tag{10}$$

This immediately concludes the proof of Lemma 1. ∎

Lemma 2. Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be $2n$-mode Gaussian states such that $\mathrm{Tr}_A |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_A |\psi_1\rangle\langle\psi_1|$, there exists a Gaussian unitary operator U acting on n modes such that $(U \otimes \mathbb{I})|\psi_0\rangle = |\psi_1\rangle$, where $\mathbb{I}$ is the identity on n modes.

In the discrete-variable case, this is a consequence of the Schmidt decomposition of $|\psi_0\rangle$ and $|\psi_1\rangle$. Here, this role is played by the *normal mode decomposition* [24]. Noting as $\mu_b = \begin{pmatrix} \mu_b^A \\ \mu_b^B \end{pmatrix}$ and $\gamma_b = \begin{pmatrix} \gamma_b^A & C_b \\ C_b^T & \gamma_b^B \end{pmatrix}$ the first- and second-order moments of $|\psi_b\rangle$, the perfectly concealing condition $\mathrm{Tr}_A |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_A |\psi_1\rangle\langle\psi_1|$ implies that $\mu_0^B = \mu_1^B$ and $\gamma_0^B = \gamma_1^B$. As a consequence, γ_0^A and γ_1^A have the same symplectic spectra, so that, by applying the normal mode decomposition on γ_0 and γ_1, we know that there exist symplectic matrices S_b^j such that

$$\gamma_0 = \left(S_0^A \oplus S_0^B\right) \tilde{\gamma} \left(S_0^A \oplus S_0^B\right)^t, \tag{11}$$

$$\gamma_1 = \left(S_1^A \oplus S_1^B\right) \tilde{\gamma} \left(S_1^A \oplus S_1^B\right)^t. \tag{12}$$

S_0^B and S_1^B can be chosen to be equal since $\gamma_0^B = \gamma_1^B$. The symplectic matrix $\mathcal{S} = S_1^A (S_0^A)^{-1} \oplus \mathbb{I}_{2n}$ transforms γ_0 into γ_1 by acting on Alice's modes only. Similarly, the displacement $\mu_1 - \mathcal{S}\mu_0$ transforms μ_0 into μ_1 by acting on Alice's side only, which proves Lemma 2. ∎

Perfectly concealing protocols. We now turn to the proof of our no-go theorem for Gaussian QBC. For perfectly concealing protocols ($\varepsilon = 0$), Alice's cheating strategy is well-known: she simply applies an appropriate unitary operation to her half of $|\psi_b\rangle$ between the two stages of the protocol. This allows her to convert $|\psi_0\rangle$ into $|\psi_1\rangle$. In the case of Gaussian QBC, Lemma 2 implies that this cheating unitary is Gaussian.

ε-concealing protocols. We now investigate the realistic case where the protocol is not perfectly concealing, which will finally lead us to the proof of Theorem 1. We want to find an explicit Gaussian $\sqrt{2\varepsilon}$-cheating strategy for Alice against a ε-concealing QBC protocol. In the first stage of the protocol, Alice creates the state $|\psi_0\rangle$ and sends ρ_0 to Bob. In the second stage, if Alice wants to reveal the bit 0, she sends her half of $|\psi_0\rangle$ to Bob, while if she decides to reveal the bit 1, she applies a Gaussian unitary operation to her half of $|\psi_0\rangle$, mapping it to $|\psi_1^\sharp\rangle$, and then sends it to Bob.

As a consequence of Lemma 1, there exist Gaussian purifications $|\hat{\psi}_0\rangle$ of ρ_0 and $|\hat{\psi}_1\rangle$ of ρ_1 such that $D(\hat{\psi}_0, \hat{\psi}_1) \leqslant \sqrt{2D(\rho_0, \rho_1)}$. Moreover $|\hat{\psi}_0\rangle$ and $|\psi_0\rangle$ ($|\hat{\psi}_1\rangle$ and $|\psi_1\rangle$) are two Gaussian purifications of the same Gaussian state ρ_0 (ρ_1), so that, according to Lemma 2, there exists Gaussian unitary operators U_0 and U_1 such that $(U_0 \otimes \mathbb{I})|\psi_0\rangle = |\hat{\psi}_0\rangle$ and $(U_1 \otimes \mathbb{I})|\psi_1\rangle = |\hat{\psi}_1\rangle$, respectively. We note that $|\psi_1^\sharp\rangle = (U_1^{-1} U_0 \otimes \mathbb{I})|\psi_0\rangle = (U_1^{-1} \otimes \mathbb{I})|\hat{\psi}_0\rangle$. By unitary invariance of the trace distance, one has $D(\psi_1^\sharp, \psi_1) = D(\hat{\psi}_0, \hat{\psi}_1)$. Thus, for ε-concealing protocols, we have $D(\psi_1^\sharp, \psi_1) \leqslant \sqrt{2\varepsilon}$, which concludes the proof of Theorem 1. ∎

We have thus obtained a stronger result than the standard no-go theorem, since we have shown that QBC remains impossible even if Alice and Bob are restricted to manipulating Gaussian states. Although Lemma 1 can be seen as a weak version of Uhlmann's theorem in the sense that the intrinsic purification does not reach Uhlmann's bound, it is sufficient here because the quantities of interest in terms of guessing probability have not changed. Interestingly, the question of whether the purifications that saturate Uhlmann's bound could both be chosen Gaussian if the states are Gaussian is still open (although partial results in this direction have been obtained in [25]). Note also that we have an explicit construction of Alice's cheating purifications for any CV QBC protocol, Gaussian or not. This is done by noting that the Gaussian constraint can be relaxed in the proof of Lemma 1, and that Lemma 2 can be replaced by the usual Schmidt decomposition.

CBH theorem. Consider the subset of quantum mechanics where only Gaussian states and operations are allowed. As a result of our no-go theorem, this Gaussian model forbids bit commitment, while it allows unconditional secret key

distribution [15]. Interestingly, however, it is strictly included in quantum mechanics since, for instance, Bell inequalities cannot be violated with Gaussian states and measurements. This contradicts the Brassard-Fuchs conjecture. Furthermore, according to the CBH theorem [11], quantum mechanics can be rederived from the sole assumptions that signaling, broadcasting, and bit commitment are impossible in Nature. While this idea is very appealing, the Gaussian model again provides a natural counter-example to it. The reason is that the CBH theorem actually requires the further assumption that the physical description of Nature is done within the framework of C^* algebras (Spekkens had found a toy model compatible with CBH but distinct from quantum mechanics [26], but ours is physically better grounded).

Conclusion. We have addressed continuous-variable quantum bit commitment and have proven a strong version of the standard no-go theorem in which Alice and Bob are restricted to Gaussian states and operations. Our proof is based on a Gaussian purification of Gaussian states, eliminating the need for Uhlmann's theorem. Note that Bob is not restricted to Gaussian measurements at the last stage of the protocol, which may make him more powerful than in a fully Gaussian protocol. Even then, Alice can always perform a Gaussian cheating strategy. This leaves open, however, the possible existence of non-Gaussian QBC protocols that could be secure against Gaussian attacks. More fundamentally, we have exhibited a physically motivated counter-example to the attempts at rederiving quantum mechanics from first principles.

We thank R. García-Patrón, A. Grinbaum, and S. Pirandola for fruitful discussions. We acknowledge financial support of the European Union under the FET projects COMPAS (212008) and QAP (015848), the Agence Nationale de la Recherche under Projects SEQURE (ANR-07-SESU-011-01), QRAC (ANR-08-EMER-012), and CRYQ (ANR-09-JCJC-460290), and the Brussels-Capital Region under Project CRYPTASC.

[1] M. Naor, J. Cryptology **4**, 151 (1991).
[2] D. Chaum, in *Advances in Cryptology—CRYPTO '86*, Lecture Notes in Computer Science, edited by A. M. Odlyzko (Springer-Verlag, London, 1987), p. 195.
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[4] G. Brassard *et al.*, in *34th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1993), p. 42.
[5] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[6] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[7] H. P. Yuen, e-print arXiv:quant-ph/0006109v7.
[8] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).
[9] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[10] G. Brassard, Nature Phys. **1**, 2 (2005).
[11] R. Clifton *et al.*, Found. Phys. **33**, 1561 (2003).
[12] I. B. Damgård *et al.*, SIAM J. Comput. **37**, 1865 (2008).
[13] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).
[14] *Quantum Information with Continuous Variables of Atoms and Light*, edited by N. J. Cerf, G. Leuchs, and E. S. Polzik (Imperial College Press, London, 2007).
[15] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[16] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[17] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[18] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[19] T. Kailath, IEEE Trans. Commun. Technol. **15**, 52 (1967).
[20] S. Pirandola and S. Lloyd, Phys. Rev. A **78**, 012331 (2008).
[21] Arvind *et al.*, Pramana **45**, 471 (1995).
[22] R. Simon *et al.*, J. Math. Phys. **40**, 3632 (1999).
[23] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[24] A. Botero and B. Reznik, Phys. Rev. A **67**, 052311 (2003).
[25] P. Marian and T. A. Marian, Phys. Rev. A **76**, 054307 (2007).
[26] R. W. Spekkens, Phys. Rev. A **75**, 032110 (2007).